Buletin Bulanan Keamanan Komputer

Punya Cadangan?

Sekilas

Bila Anda pengguna komputer atau gawai/alkom sejak lama, cepat atau lambat pasti mengalami sebuah ketidak-nyamanan. Bisa saja tidak sengaja keliru dalam menghapus berkas,rusak atau bahkan hilangnya peralatan. Malah terkadang malware atau ransomware "menyandera" berkas Anda. Dalam situasi seperti ini, cadangan hanya merupakan satu-satunya cara untuk membangun kembali kehidupan digital Anda.

Apa, Kapan dan Bagaimana

Cadangan adalah salinan informasi yang disimpan di tempat/lokasi lain di luar perangkat komputer atau gawai Anda. Saat sebuah data penting hilang, data tersebut bisa diunduh- ulang dari cadangan. Untuk itu langkah pertama adalah menentukan apa saja yang mesti dicadangkan; (1) data penting tertentu saja atau (2) semuanya, termasuk seluruh sistem operasi. Solusi pencadangan biasanya menggunakan cara pertama, jadi hanya melakukan pencadangan untuk folder yang sering digunakan. Bila ragu mana yang penting atau ingin extra hati-hati, lakukan pilihan kedua.

Kedua, tentukan seberapa sering pencadangan perlu dilakukan. Beberapa perangkat lunak seperti Apple's Time Machine atau Windows Backup and Restore memungkinkan mengatur jadwal itu secara mudah. Umumnya ada pilihan dalam skala jam, harian, mingguan dll. Solusi lain adalah menerapkan solusi berkelanjutan, artinya setiap ada berkas baru atau berkas yang diubah, sistem akan langsung membuat cadangannya. Gampangnya, setidaknya lakukan pencadangan harian pada berkas-berkas penting.

Setelah itu, tentukan bagaimana proses pencadangan akan dilakukan. Ada dua pilihan: disimpan lokal atau cloud. Pencadangan lokal bergantung pada peralatan umum seperi USB Drives atau peralatan penyimpanan yang terhubung ke Wifi. Kelebihan sistem ini adalah kemudahan dalam melakukan pencadangan dan unduh ulang (recover) data dalam jumlah besar secara cepat. Kelemahannya, bila tertular malware seperti ransomware, bisa saja cadangan juga ikut tertular. Selain itu, bila ada resiko kebakaran atau pencurian, Anda beresiko kehilangna komputer dan mungkin juga cadangannya. Untuk itu, bila menggunakan peralatan external untuk pencadangan, simpan ditempat aman dan lakukan pelabelan/penamaan dengan akurat.

Solusi berbasis cloud pada dasarnya adalah jasa daring penyimpanan berkas via internet. Diawali dengan instalasi aplikasi di komputer, selanjutnya aplikasi ini secara otomatis akan melakukan proses pencadangan berkas sesuai jadwal. Cara ini cukup

sederhana, pencadangan berjalan secara otomatis dan berkas bisa diakses dari mana saja. Tambahan lagi, karena berkas disimpan di cloud, resiko adanya kebakaran atau pencurian bisa dihindari. Selain itu pencadangan di cloud lebih memberikan keamanan saat unduh-ulang setelah infeksi malware. Hanya saja, keleluasaan melakukan pencadangan ditentukan oleh besaran/ volume data dan kecepatan jaringan. Tidak yakin solusi mana yang akan dipilih? Kalau mau extra aman, gunakan keduanya.

Data di gawai biasanya sudah disimpan di cloud. Namun, konfigurasi aplikasi, foto terbaru dan pengaturan preferensi mungkin belum tersimpan di cloud. Dengan melakukan pencadangan gawai/alkom, Anda tidak hanya menyimpam informasi diatas namun memudahkan juga saat memindahkan data bila terjadi penggantian atau peralatan baru.

Catatan Tambahan

- **Pencadangan dan unduh-ulang adalah sama-sama penting. Kedua hal itu harus dipastikan kesuksesannya. Lakukan tes unduh-ulang dari berkas cadangan. Pastikan apa yang sudah dicadangkan bisa dibaca dengan baik dan benar.**
- **Bila melakukan configurasi ulang dari sistem cadangan, pastikan melakukan pembaruan (patches dan update) secara menyeluruh sebelum menggunakannya**
- **Dalam menentukan solusi cloud, pilih yang gampang digunakan dan perhatikan pula opsi keamanannya. Contoh: Apakah ada pilihan verifikasi dua tahap untuk menjaga keamanan akun daring Anda.**

Pencadangan adalah cara mudah dan ekonomis bagi perlindungan dunia digital Anda.

Versi Bahasa Indonesia

BIPIMax memberikan Pelatihan Optimasi Proses Bisnis (LSS) dan Pengenalan Keamanan & Proteksi Informasi. Informasi lengkap: http://www.bipimax.net

Editor Tamu

Matt Bromiley *adalah seorang ahli di bidang keamanan siber dan unit reaksi insiden di berbagai organisasi. Sebagai seorang pengajar di SANS, dengan bidang spesialisasi pelaporan dan reaksi insiden serta penelusuran ancaman, FOR508 dan FOR572. Hadir di Twitter sebagai* @mbromileyDFIR.

Sumber Pustaka

Making Passwords Simple: https://www.sans.org/u/TqR

Menangkal Malware: https://www.sans.org/u/TqW

Hadirkan Dunia Siber Aman di Rumah: https://www.sans.org/u/Tr1